

U.S. Department of Housing and Urban Development

OSPM

HUDStat

Privacy Impact Assessment

1/21/2011

DOCUMENT ENDORSEMENT

I have carefully assessed the Privacy Impact Assessment (PIA) for **[Insert Name of IT System and/ or Information Collection Request]**. This document has been completed in accordance with the requirement set forth by the [E-Government Act of 2002](#) and [OMB Memorandum 03-22](#) which requires that "Privacy Impact Assessments" (PIAs) be conducted for all new and/ or significantly altered IT Systems, and Information Collection Requests.

ENDORSEMENT SECTION

Please check the appropriate statement.

 x **The document is accepted.**
 The document is accepted pending the changes noted.
 The document is not accepted.

Based on our authority and judgment, the data captured in this document is current and accurate.

/s/ Peter Grace

SYSTEM OWNER
[PROGRAM OFFICE]

11/2/11

Date

/Sara Meyers/

PROGRAM AREA MANAGER
[PROGRAM OFFICE]

11/2/11

Date

/Harold Williams/

DEPARTMENTAL PRIVACY ACT OFFICER
Office of the Chief Information Officer
U. S. Department of Housing and Urban Development

11/3/11

Date

TABLE OF CONTENTS

DOCUMENT ENDORSEMENT	2
ENDORSEMENT SECTION	2
TABLE OF CONTENTS	3
SECTION 1: BACKGROUND.....	4
Importance of Privacy Protection – Legislative Mandates:	4
What is the Privacy Impact Assessment (PIA) Process?	5
Who Completes the PIA?.....	5
When is a Privacy Impact Assessment (PIA) Required?.....	5
What are the Privacy Act Requirements?	6
Why is the PIA Summary Made Publicly Available?	6
SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT.....	7
Question 1: Provide a brief description of what personal information is collected.....	7
Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?	9
Question 3: Type of electronic system or information collection.....	9
Question 4: Why is the personally identifiable information being collected? How will it be used?	11
Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose or outside the government)?	12
Question 6: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?	12
Question 6: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?.....	13
Question 7: If privacy information is involved, by what data element(s) is it retrieved from the system?.....	14
SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER.....	14

**U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
PRIVACY IMPACT ASSESSMENT (PIA) FOR:
[“HUDSTAT”]**

**(for IT Systems: [Insert OMB Unique Identifier]
and PCAS: 411750)**

6/25/10

NOTE: See Section 2 for PIA answers, and Section 3 for Privacy Act Officer’s determination.

SECTION 1: BACKGROUND

Importance of Privacy Protection – Legislative Mandates:

HUD is responsible for ensuring the privacy and confidentiality of the information it collects on members of the public, beneficiaries of HUD programs, business partners, and its own employees. These people have a right to expect that HUD will collect, maintain, use, and disseminate identifiable personal information only as authorized by law and as necessary to carry out agency responsibilities.

The information HUD collects is protected by the following legislation and regulations:

- [Privacy Act of 1974, as amended](#) affords individuals the right to privacy in records that are maintained and used by Federal agencies. (See <http://www.usdoj.gov/foia/privstat.htm>; see also [HUD Handbook 1325.1 at www.hudclips.org](#));
- Computer Matching and Privacy Protection Act of 1988 is an amendment to the Privacy Act that specifies the conditions under which private information may (or may not) be shared among government agencies. (See <http://www.usdoj.gov/foia/privstat.htm>);
- [Freedom of Information Act of 1966, as amended](#) (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm) provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy. See also [HUD’s Freedom of Information Act Handbook \(HUD Handbook 1327.1 at www.hudclips.org\)](#);
- [E-Government Act of 2002](#) requires Federal agencies to conduct Privacy Impact Assessments (PIAs) on its electronic systems. (See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf; see also the summary of the E-Government Act at http://www.whitehouse.gov/omb/egov/pres_state2.htm);
- [Federal Information Security Management Act of 2002](#) (which superseded the Computer Security Act of 1987) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, etc. See also the codified version of Information Security regulations at [Title 44 U.S. Code chapter 35 subchapter II \(http://uscode.house.gov/search/criteria.php\)](#); and

- [OMB Circular A-130, Management of Federal Information Resources, Appendix I](http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) (http://www.whitehouse.gov/omb/circulars/a130/appendix_i.pdf) defines Federal Agency responsibilities for maintaining records about individuals.

Access to personally identifiable information will be restricted to those staff that has a need to access the data to carry out their duties; and they will be held accountable for ensuring privacy and confidentiality of the data.

What is the Privacy Impact Assessment (PIA) Process?

The Privacy Impact Assessment (PIA) is a process that evaluates issues related to the privacy of personally identifiable information in electronic systems. See background on PIAs and the 7 questions that need to be answered, at: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>. Personally identifiable information is defined as information that actually identifies an individual, e.g., name, address, social security number (SSN), or identifying number or code; or other personal/ sensitive information such as race, marital status, financial information, home telephone number, personal e-mail address, etc. Of particular concern is the combination of multiple identifying elements. For example, knowing name + SSN + birth date + financial information would pose more risk to privacy than just name + SSN alone.

The PIA:

- Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to HUD's mission is included.

Who Completes the PIA?

Both the program area System Owner and IT Project Leader work together to complete the PIA. The System Owner describes what personal data types are collected, how the data is used, and who has access to the personal data. The IT Project Leader describes whether technical implementation of the System Owner's requirements presents any risks to privacy, and what controls are in place to restrict access of personally identifiable information.

When is a Privacy Impact Assessment (PIA) Required?

- 1. New Systems:** Any new system that will contain personal information on members of the public requires a PIA, per OMB requirements (this covers both major and non-major systems).
- 2. Existing Systems:** Where there are significant modifications involving personal information on members of the public, or where significant changes been made to the system that may create a new privacy risk, a PIA is required.

3. Information Collection Requests, per the Paperwork Reduction Act (PRA):

Agencies must obtain OMB approval for new information collections from ten or more members of the public. If the information collection is both a new collection and automated, then a PIA is required.

What are the Privacy Act Requirements?

Privacy Act. The [Privacy Act of 1974](http://www.usdoj.gov/foia/privstat.htm), as amended (<http://www.usdoj.gov/foia/privstat.htm>) requires that agencies publish a Federal Register Notice for public comment on any intended information collection. Privacy Act Systems of Records are created when information pertaining to an individual is collected and maintained by the Department, and is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to an individual. The [E-Government Act of 2002](#) requires PIAs for electronic systems as well as information collection requests that are automated. So, there is a relationship between the new PIA requirement (when automation is involved) and the long-standing Privacy Act System of Records Notices (for both paper-based and automated records that are of a private nature). For additional information, contact the Departmental Privacy Act Officer in the Office of the Chief Information Officer.

Why is the PIA Summary Made Publicly Available?

The E-Government Act of 2002 requires that the analysis and determinations resulting from the PIA be made publicly available. The Privacy Advocate in HUD's Office of the Chief Information Officer (OCIO) is responsible for publishing the PIA summary on HUD's web site. See: <http://www.hud.gov/offices/cio/privacy/pia/pia.cfm>.

SECTION 2 – COMPLETING A PRIVACY IMPACT ASSESSMENT

Please submit answers to the Departmental Privacy Act Officer in the Office of the Chief Information Officer (OCIO). If any question does not apply, state Not Applicable (N/A) for that question, and briefly explain why it is not applicable.

Program Area: Office of Strategic Planning and Management (DEPSEC)

Subject matter expert in the program area: Sara Meyers

Program Area Manager: Peter Grace

IT Project Leader: Badeah Carroll

For IT Systems:

- **Name of system:** HUDStat
- **PCAS #:** 411750
- **OMB Unique Project Identifier #:** Will be provide during production phase
- **System Code:** P275
- **Development Date:** Not applicable to pilot
- **Expected Production Date:** 3/31/11

For Information Collection Requests:

- **Name of Information Collection Request:**
- **OMB Control #:**

Question 1: Provide a general description of the system that describes: (a) the personal information collected; (b) who does it pertain only to (i.e., government employees, contractors, or consultants); (c) the functionality of the system and the purpose that the records and/or system serve; (d) how information is transmitted to and from the system; (e) interconnections with other systems.

The purpose of HUDStat phase 1 is to measure progress towards strategy goals, by integrating grantee data from across the agency; and to allow the Department to determine how well investments are performing as a whole and how targets for measuring these goals are being met.

Phase 1 of HUDStat will be a rapid deployment of a subset of Strategic Plan's Key Measures of Success: The High Priority Performance Goals (HPPGs). There will be no interconnections with other systems involved; data will be manually extracted from program system by program staff and email to database administrators. The Department systems for which extracts are received from are: Single Family Data Warehouse; CFO DataMart; Policy Development and Research data sources; Electronic Special Needs Assistance Program System; Recovery Act Management and Performance System; Integrated Disbursement and Information System; Quarterly Performance and Evaluation Reporting System; Integrated Real Estate Management System. The measures supporting HPPG are Foreclosure Prevention, Rental Assistance, Veteran's Homelessness, and Energy Retrofits, which will involve aggregate data at the project level only such as number of units, summary of funding, number of affected homeowners, and number and type of energy efficiency improvements completed.

The HUDStat PIA will be revisited and updated during the requirement definition phase to expand on the systems usability and to incorporate any changes

If this automated system (or Information Collection Request) involves personally identifiable information on members of the public, then **mark any of the categories that apply below:**

Personal Identifiers:

	Name
	Social Security Number (SSN). Specify the purpose/legal authority authorizing the solicitation of SSNs (This includes truncated SSNs):
X	Other identification number (specify type): Case number from the Single Family Data Warehouse. There is no way to identify the individuals associated with the cases within the HUDStat system because the case number is not used anywhere else in the system, and because HUDStat does not store the personal information associated with the case number.
	Birth date
X	Home address: Will not collect information that identifies individuals. Only multifamily property locations (already stored in other systems) or non-PII address info (ie census tracts) will be used.
	Home telephone
	Personal e-mail address
	Fingerprint/ other "biometric"
	Other (specify):
	None
	Comment:

Personal/ Sensitive Information:

	Race/ ethnicity
	Gender/ sex
	Marital status
	Spouse name
	# of children
	Income/ financial data (specify type of data, such as salary, Federal taxes paid, bank account number, etc.):
	Employment history:
	Education level
	Medical history/ information
	Disability
	Criminal record
	Other (specify):
	None
	Comment:

Question 2: Will any of the personally identifiable information be accessed remotely or physically removed?

	Yes	No
If yes, Proceed to answering the following questions.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Have the security controls been reviewed and approved by the Information Security Officer?	<input type="checkbox"/>	<input type="checkbox"/>
What security controls are in place to protect the information (e.g., encryptions)?		
What HUD approved application is used to grant remote access (e.g., VPN, Citrix)?		
Is there a policy in place restricting remote access from certain locations outside the Department (For example: Policy may permit remote access, but prohibits access from a particular place; such as, Kinko's/Starbuck) or is remote access permitted from all areas outside the Department?		
Is there a policy that identifies "if" or "if not" downloading and remote storage of this information is allowed (For example: Policy may permit remote access, but prohibit downloading and local storage)?		
Comment:		

Question 3: Type of electronic system or information collection.

	Yes	No
A. If a new electronic system (or one in development) (implemented after April 2003, the effective date of the E-Government Act of 2002)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Does the system require authentication?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system browser-based?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the system external-facing (with external users that require authentication)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

	Yes	No
B. If this is existing electronic system has the system undergone any changes (since April 17, 2003)? If an existing system, when was the system developed? _____	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?	<input type="checkbox"/>	<input type="checkbox"/>
Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?	<input type="checkbox"/>	<input type="checkbox"/>
If yes, please explain:		

C. For your new and/or existing electronic system, please indicate if any of the following changes have occurred: Mark any of the following conditions for your existing system that OMB defines as a “trigger” for requiring a PIA or PIA update (if not applicable, mark N/A):	
NA	Conversion: When paper-based records that contain personal information are converted to an electronic system
NA	From Anonymous (Non-Identifiable) to “Non-Anonymous” (Personally Identifiable): When any systems application transforms an existing database or data collection so that previously anonymous data becomes personally identifiable
NA	Significant System Management Changes: When new uses of an existing electronic system significantly change how personal information is managed in the system. (Example #1: when new “relational” databases could combine multiple identifying data elements to more easily identify an individual. Example #2: when a web portal extracts data elements from separate databases, and thereby creates a more open environment for exposure of personal data)
NA	Merging Databases: When government databases are merged, centralized, matched, or otherwise significantly manipulated so that personal information becomes more accessible (with special concern for the ability to combine multiple identifying elements)
NA	New Public Access: When <u>new</u> public access is given to members of the public or to business partners (even if the system is protected by password, digital certificate, or other user-authentication technology)
NA	Commercial Sources: When agencies systematically incorporate into databases any personal data from commercial or public sources (ad hoc queries of such sources using existing technology does not trigger the need for a PIA)
NA	New Inter-agency Uses: When agencies work together (such as the federal E-Gov initiatives), the lead agency should prepare the PIA
NA	Business Process Re-engineering: When altering a business process results in significant new uses, disclosures, or additions of personal data.
NA	Alteration in Character of Data: When adding new personal data raises the risks

	to personal privacy (for example, adding financial information to an existing database that contains name and address)
--	--

D. If an Information Collection Request (ICR): Is this a <u>new</u> Request that will collect data that will be in an <u>automated</u> system? Agencies must obtain OMB approval for information collections from 10 or more members of the public. The E-Government Act of 2002 requires a PIA for ICRs only if the collection of information is a <u>new</u> request and the collected data will be in an <u>automated</u> system.	
	Yes, this is a new ICR and the data will be automated
X	No, the ICR does not require a PIA because it is not <u>new</u> or <u>automated</u>
	Comment:

Question 4: Explain by Line of Business why the personally identifiable information being collected? How will it be used?

Mark any that apply:

Homeownership:

	Credit checks (eligibility for loans)
	Loan applications and case-binder files (via lenders) – including borrower SSNs, salary, employment, race, and other information
	Loan servicing (MIP collections/refunds and debt servicing for defaulted loans assigned to HUD)
	Loan default tracking
	Issuing mortgage and loan insurance
	Other (specify):
	Comment:

Rental Housing Assistance:

	Eligibility for rental assistance or other HUD program benefits
	Characteristics on those receiving rental assistance (for example, race/ethnicity, # of children, age)
	Property inspections
	Other (specify):
	Comment:

Grants:

	Grant application scoring and selection – if any personal information on the grantee is included
	Disbursement of funds to grantees – if any personal information is included
	Other (specify):
	Comment:

Fair Housing:

	Housing discrimination complaints and resulting case files
	Other (specify):
	Comment:

Internal operations:

	Employee payroll or personnel records
	Payment for employee travel expenses
	Payment for services or products (to contractors) – if any personal information on the payee is included
	Computer security files – with personal information in the database, collected in order to grant user IDs
	Other (specify):
	Comment:

Other lines of business (specify uses):

X	Nothing new will be collected for this release, but locations and/or case numbers may be used to identify trends by location and unique counts.

Question 5: Will you share the information with others? (e.g., another agency for a programmatic purpose, internal HUD application/module or outside the government)?

Mark any that apply:

	Federal agencies?
	State, local, or tribal governments?
	Public Housing Agencies (PHAs) or Section 8 property owners/agents?
	FHA-approved lenders?
	Credit bureaus?
	Local and national organizations?
	Non-profits?
	Faith-based organizations?
	Builders/ developers?
	HUD module/application? (specify the module(s)/application(s) name) ALL
	Others? (specify):
	Comment:

Question 6: Can individuals “opt-out” by declining to provide personal information or by consenting only to particular use (e.g., allowing their financial information to be used for basic rent eligibility determination, but for not for sharing with other government agencies)?

	Yes, they can “opt-out” by declining to provide private information or by consenting only to particular use
	No, they can’t “opt-out” – all personal information is required
	Comment:

If Yes, please explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data):

Question 7: How will the privacy of the information be protected/ secured? What are the administrative and technological controls?

Mark any that apply and give details if requested:

X	System users must log-in with a password (Please specify password type): Password will be authenticated by active directory service. This service utilizes current HUD policy to enforce password strength, minimum password length, password history, password aging, and invalid login attempts (lockout).
X	When an employee leaves: <ul style="list-style-type: none"> • How soon is the user ID terminated? (1 day, 1 week, 1 month, unknown)? • How do you know that the former employee no longer has access to your system? (explain your procedures or describe your plan to improve): User access and termination is controlled through HUD’s CHAMP process. As employees leave HUD, supervisors are required to submit CHAMP requests to delete ALL access by the departing user. As part of the CHAMP workflow process, the system SSA will remove the user’s access. Also, once the user’s access has been removed from active directory, the user will no longer be able to access the system.
X	Are access rights selectively granted, depending on duties and need-to-know? If Yes, specify the approximate # of authorized users who have either: <ul style="list-style-type: none"> • Full access rights to all data in the system: 15 Limited/restricted access rights to only selected data: 300
X	Are disks, tapes, and printouts that contain personal information locked in cabinets when not in use? (explain your procedures, or describe your plan to improve): Reports do not contain personally identifiable information.
	If data from your system is shared with another system or data warehouse, who is responsible for protecting the privacy of data that came from your system but now resides in another? Explain the existing privacy protections, or your plans to improve: No data is shared with other systems.
	Other methods of protecting privacy (specify):
	Comment:

Question 8: If privacy information is involved, by what data element(s) is it retrieved from the system?

Mark any that apply

	Name:
	Social Security Number (SSN)
	Identification number (specify type):
	Birth date
	Race/ ethnicity
	Marital status
	Spouse name
	Home address
	Home telephone
	Personal e-mail address
	Other (specify):
X	None
	Comment:

Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the Federal Register to cover this system? Yes ☐ No ☒ (Please consult with your component's Privacy office if assistance is needed in responding to this question.)

If yes, provide the Federal Register citation

Other Comments (or details on any Question above):

We will update this document for pilot phase 2 as well as for the long term project.

SECTION 3: DETERMINATION BY HUD PRIVACY ACT OFFICER

The Privacy Office examined the programs HUDStat PIA responses and has determined that there are no privacy related risks at this time. The 1st pilot phase will not collect, maintain, or disseminate any PII and/or the eventual 2nd phase or long term project will most likely not collection this information. If decisions change concerning the collection of PII the program sponsor will consult with Privacy Office beforehand to ensure that all privacy related requirement are addressed. Program Officials will revisit the PIA and make necessary updates concerning the long term project activities.